La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux

6 | 2014
Revue des droits de l'homme - N° 5

Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point

Clémentines Bories

OpenEdition Journals

Electronic version
URL: http://journals.openedition.org/revdh/984
DOI: 10.4000/revdh.984
ISSN: 2264-119X

Publisher
Centre de recherches et d'études sur les droits fondamentaux

Electronic reference
Clémentines Bories, « Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point », *La Revue des droits de l'homme* [Online], 6 | 2014, Online since 04 December 2014, connection on 08 July 2020. URL : http://journals.openedition.org/revdh/984 ; DOI : https://doi.org/10.4000/revdh.984

Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point

Clémentines Bories

1 « Une clef USB défaillante peut faire plus de dégâts qu'une bombe de 250 kg ». A en croire le général Eric Bonnemaison, Directeur adjoint des Affaires stratégiques au Ministère de la Défense, la menace informatique, non contente de bouleverser le visage des conflits armés classiques, constituerait un risque fondamental pour les Etats ainsi que les civils. La « cyberguerre » est un phénomène relativement neuf, dont l'apparition se justifie par notre dépendance à l'outil informatique mais aussi par le faible coût qu'il y a à faire d'un instrument de communication et de travail une arme immatérielle dotée d'un fort potentiel offensif. Phénomène devenu d'ampleur dans les relations internationales et impliquant au premier chef les Etats Unis d'Amérique, la Chine et la Russie, la « cyberguerre » constitue à la fois une déclinaison nouvelle des tensions internationales et un enjeu pour le droit. Ce n'est que depuis peu qu'elle préoccupe les juristes[1], et ce surtout en dehors de nos frontières. Les analyses se concentrent alors avant tout sur les modifications du *jus in bello* et du *jus ad bellum* qui pourraient s'avérer nécessaires. La question de l'opportunité d'un traité international régissant les conflits informatiques est notamment discutée, mais ne paraît pas susceptible de donner lieu à une réalisation véritable dans un délai raisonnable[2].

2 Il apparaît dès lors opportun d'interroger le droit positif afin de cerner comment les règles en vigueur peuvent permettre d'envisager les actions informatiques offensives. La présente étude se concentrera non sur les actes de piraterie informatique qui sont le fait d'individus isolés mais sur celles des actions informatiques offensives qui impliquent des Etats, en qualité de commanditaire ou bien de cible, ou encore parce que leurs ressortissants sont les victimes. Apparaît alors une première difficulté, d'ordre non seulement sémantique mais aussi conceptuel : ladite « cyberguerre », multifacettes, doit être définie afin que l'objet de l'analyse puisse être véritablement déterminé (I). Suit une seconde difficulté, celle de l'identification de règles de droit

international permettant de répondre aux enjeux de telles attaques en protégeant les victimes civiles, tout en désignant les éventuels Etats commanditaires et/ou victimes de tels agissements (II).

I – Des phénomènes nouveaux à appréhender

3 Parce que le terme de « cyberguerre » est utilisé à tort et à travers pour désigner des faits avérés ou fantasmés, il s'avère que les phénomènes qu'il désigne, hétéroclites (A), ne se prêtent pas à une appréhension aisée par le biais d'un concept juridique unique (B).

A – L'hétérogénéité des situations de fait concernées

4 Alors pourtant qu'elle constituait l'objet même de son mandat, le General Keith B. Alexander (USA), Director of the NSA and Commander of the US CyberCommand (CYBERCOM) soulignait, dans un discours au Sénat prononcé en 2013, la totale imprécision de la définition du terme de cyberguerre : « qu'est-ce qui constitue un acte de guerre dans le cyberespace ? ». Il est vrai que le terme de « cyberguerre », sur-employé sans doute à la fois par commodité et en raison de son caractère frappant, renvoie à des réalités fort différenciées et difficilement saisissables. Dépourvu d'acception juridique assurée, le néologisme devenu fréquent fait référence, dans son acception courante, à des situations de fait dans lesquelles l'outil informatique est utilisé aux fins de créer un dommage dans une sphère internationale, sans nécessairement avoir recours à la violence. S'inscrivant dans un contexte conflictuel ou simplement hostile voire suspicieux, tantôt dans le cadre des relations internationales, tantôt au sein même du territoire d'un Etat, les actes de cyberguerre peuvent survenir dans de multiples configurations.

5 Entendue *stricto sensu*, la cyberguerre devrait n'être que virtuelle, ne faire appel qu'à des armes électroniques[3], et n'être conduite que dans une sphère immatérielle. Au-delà de ce cas d'école[4] et de façon plus habituelle, un acte de cyberguerre peut consister dans une opération menée dans le cadre d'un conflit armé avéré, qu'il soit international ou interne ; c'est ainsi dans le contexte de la Guerre d'Ossétie du Sud que se sont inscrites les attaques russes visant la Géorgie (2008). Plus fréquemment, l'acte dit de cyberguerre intervient en dehors de tout conflit armé, ne correspond ni à la guerre ni à la paix mais se trouve « *somewhere between* »[5]. Une attaque électronique commanditée par des autorités étatiques soucieuses de porter atteinte aux intérêts d'une Puissance étrangère peut être décrite comme un acte de « cyberguerre ». Il s'agit là de l'hypothèse sans doute la plus communément référencée, qui concerna par exemple l'Estonie, victime en avril 2007 d'opérations de grande ampleur qui ont, en plusieurs étapes, touché les sites gouvernementaux, les banques, les media et les partis politiques, jusqu'à paralyser le gouvernement. L'action informatique pourra s'inscrire dans le cadre de relations internationales tendues et correspondre à des actions hostiles dirigées contre un autre Etat, à l'instar des attaques pro-taiwanaises dirigées contre les sites gouvernementaux chinois en 1999 ou des attaques commanditées la même année par le Gouvernement chinois à l'encontre des Etats-Unis d'Amérique en réponse au bombardement accidentel de l'Ambassade chinoise à Belgrade. Comme en atteste les politiques américaine et israélienne à l'égard de l'Iran ainsi que

l'opération Stuxnet menée contre des installations nucléaires, il peut également correspondre à une politique de dissuasion voire à une contre-mesure. Est également désignée par le vocable « cyberguerre » toute action informatique hostile susceptible de déclencher un conflit armé.

6 Plus largement, dans le langage courant, l'appellation « cyberguerre » peut désigner une opération menée par un Etat à l'encontre d'une entité non étatique en dehors de son territoire, notamment dans le cadre de la lutte contre le terrorisme, ou encore une offensive terroriste menée à l'initiative d'un groupe non étatique mais destinée à porter atteinte aux intérêts d'un Etat ou de sa population[6]. Une action entreprise à l'initiative d'autorités étatiques à l'encontre d'un groupe hostile situé sur leur territoire et ayant par exemple proclamé son indépendance pourra elle aussi être incluse parmi les actes dits de « cyberguerre ». Enfin, et suivant une interprétation sans doute démesurément extensive de l'expression de « cyberguerre », pourrait être concernée une cyber-révolution impulsée par réseaux sociaux incitant à la violence ou au changement de régime politique, telle la Révolution tunisienne de 2011 qui bénéficia de l'aide apportée par les Anonymous.

B – Une qualification juridique introuvable ?

7 Une telle diversité de situations révèle les difficultés et, surtout, l'extrême limitation du phénomène étudié à laquelle conduit habituellement la considération des seules hypothèses susceptibles d'être appréhendées par le biais du droit international humanitaire. Dès lors, toute piste pour un traitement global et adapté de la question paraît opportune. Le terme de « cyberguerre » paraît bien souvent usurpé[7]. Il renvoie aux actes inamicaux visant un Etat et lui occasionnant un dommage directement ou dans la personne de ses ressortissants. Une interrogation sémantique apparaît alors : le juriste doit-il conserver le terme médiatique et courant de « cyber*guerre* » pour désigner chacun de ces phénomènes, souvent isolés et fort variés ? En effet, le conflit armé ne constitue nullement un contexte nécessaire à la survenance des faits étudiés. Dans un tel contexte, il convient d'interroger le terme composé de « cyber-guerre » pour jauger la capacité de sa composante belliqueuse à désigner, en droit, des réalités somme toute peu classiques.

8 Comme chacun sait, la qualification juridique de « conflit armé » n'est pas sans soulever nombre de difficultés d'interprétation. Pourtant, elle a d'ores et déjà été privilégiée afin de faire primer une approche compréhensive de phénomènes trop étroitement envisagés sous l'angle de la qualification de « guerre »[8]. Présenté dans l'affaire *Tadić* comme existant « à chaque fois qu'il y a recours à la force armée entre Etats ou un conflit armé prolongé entre les autorités gouvernementales et des groupes armés organisés ou entre de tels groupes au sein d'un Etat »[9], le conflit armé ainsi entendu s'écarte manifestement de la réalité des phénomènes étudiés. Certes, le conflit armé s'est par la suite présenté sous d'autres traits. Certes, face au phénomène terroriste et à la criminalité organisée[10], l'élasticité de la qualification de « guerre » a d'ores et déjà été interrogée tant sous l'angle de la définition des limites du champ d'application du *jus in bello* que de celles du *jus ad bellum*. Pourtant, rien n'est établi en droit positif qui permette une acception suffisamment large pour inclure toutes les réalités des actions informatiques. Pis, « *[t]he use of terms of war in cyberspace operations obscures the reality that cyberwar does not fit well into the legal frameworks on war and of use of force* »[11].

9 Si le terme de « guerre » permet de souligner la gravité des actes concernés et de leurs conséquences, il ne saurait, dans son acception habituelle, désigner, dans la plupart des cas, les situations d'espèce concernées par les cyber-offensives. Celles-ci se caractérisent en effet par des cibles comme des dommages d'une gravité variable, et déclinent leurs effets dans les domaines économiques, politiques, comme militaires et/ou humains. De surcroît, l'observation des faits montre que les attaques informatiques en question constituent bien souvent un moyen d'action isolé[12]. En présence de telles difficultés apparaît donc l'opportunité du recours à un autre vocable de portée générique, susceptible d'être moins controversé mais également plus neutre du point de vue du droit applicable.

10 Suivant une démarche similaire, le Center for Security Studies (CSS) de Zurich distingue d'ailleurs ces situations de celles de « cyberhacktivisme » ou « cybervandalisme » (piratage des sites avec destruction de données informatiques), du cyberterrorisme, du cybercrime et du cyberespionnage[13]. Le conflit armé seul paraît susceptible d'emporter la qualification de cyberguerre, les autres termes étant destinés à couvrir d'autres réalités.

11 C'est une autre grille de lecture que doit adopter quiconque recherche un terme permettant de désigner ensemble tous les types d'agissements dommageables, via internet, que ceux-ci soient dirigés contre un Etat ou portent atteinte à ses intérêts, et/ou soient susceptibles d'être reliées à l'action d'un autre Etat. Le cybervandalisme, le cyberterrorisme, le cyberespionnage voire, dans le cadre de la Convention sur la cybercriminalité[14] par exemple, le cybercrime, doivent pouvoir être inclus dans une qualification unique. Le terme de « cyberattaque » s'avère alors pertinent. Il permet de désigner l'une de ces pratiques, quelle qu'elle soit, dès lors qu'elle survient généralement de façon isolée et ne revêt pas toujours en elle-même la gravité suffisante pour justifier que l'on parle de « conflit armé ». L'expression « cyberattaque » fait référence à un événement plus ponctuel que celle de « cyberguerre », à un fait non nécessairement susceptible d'être qualifié d'« agression » au sens du droit international[15], et reflète dès lors plus fidèlement la palette des réalités concernées. Si les cyberopérations « peuvent être décrites au sens large comme des opérations dirigées contre un ordinateur ou un réseau informatique, ou par le biais de ceux-ci, grâce à des flux de données »[16], les cyberattaques en sont une déclinaison ; elles surviennent dans l'hypothèse où un Etat est à l'origine d'un agissement délibérément agressif à l'encontre d'intérêts politiques, militaires, économiques et commerciaux, voire sociaux.

II. Des règles à identifier

12 Une fois perçue la diversité des événements susceptibles de survenir, le juriste se doit de s'interroger sur le droit applicable à ces phénomènes tant nouveaux que disparates. Force est alors de constater le caractère partiel du raisonnement qui consiste à analyser ces événements sous l'angle classique du droit international humanitaire et du droit international général (A) ; d'autres droits pourraient recéler des clefs pour une régulation plus aisée de ces différentes situations, en particulier le droit international des droits de l'homme (B).

A – Le nécessaire dépassement des approches classiques

13 En soi, en raison de ses particularités mêmes, la cyberguerre défie les règles de droit. L'apparition de l'outil internet et des mouvements dématérialisés qu'il génère a immédiatement interrogé les juristes[17]. Si l'internet fait surgir des interrogations nouvelles pour le droit, il appelle des règles particulières. Aussi les cyberattaques dans leur diversité se caractérisent-elles par un besoin de normativité spécifique, propre à une réalité aussi difficile à localiser qu'éphémère. Davantage que le recours à des règles ponctuelles préexistantes, les cyberattaques appellent un traitement général adapté aux singularités que constituent l'usage de l'outil internet, la dématéralisation qu'il implique, l'immédiateté, ainsi que les difficultés de preuve et de localisation[18]. Mais en l'absence de telles règles spéciales, les normes susceptibles d'être applicables sont, pour l'heure, tirées principalement des droits international humanitaire et général.

14 Face à ce qu'elle désigne sous le vocable de « cyberguerre », la doctrine, à l'instar des commandements militaires, adopte habituellement un raisonnement par mimétisme avec le cas des conflits armés classiques, qui conduit à rechercher principalement l'application du droit international humanitaire. Un rapide recensement des hypothèses concernées par ladite cyberguerre permet pourtant de souligner l'insuffisance des approches qui consistent à n'analyser que l'application à ces événements de règles du *jus in bello*.

15 Si une cyberattaque implique des autorités étatiques et est susceptible d'engager leur responsabilité – ou concerne des dommages subis par elles -, les règles mobilisables dépendent du contexte factuel précis de chaque espèce. Lorsque le conflit armé est d'ores et déjà présent, le droit international humanitaire s'efforce d'appréhender la cyberattaque par le biais de ses règles[19]. Mais puisque la guerre constitue le « fait-condition » à l'applicabilité des droits de La Haye et de Genève[20], seule la cyber-« guerre » peut être appréhendée par leur biais ; le droit humanitaire est donc loin de couvrir toutes les situations de fait. De plus, lorsqu'il s'avère applicable, le *jus in bello* se heurte à moult difficultés : inexistence de règles spécifiques, et plus largement déterritorialisation de l'attaque, rareté de l'implication directe d'un Etat. Ainsi, quand bien même ses règles pourraient être utiles pour appréhender les cyberattaques, elles ne sauraient suffire à appréhender ces réalités.

16 Le droit international général, pour sa part, offre quelques pistes de solution, mais soulève, à bien y regarder, autant de questions qu'il n'en résout. Lorsque la cyberattaque constitue un recours à la force au sens du droit international, et plus précisément de la Charte des Nations Unies, elle peut au moins partiellement être appréhendée sur cette base, et qualifiée d'agression[21]. Lorsqu'enfin la cyberattaque intervient à titre de rétorsion ou de contre-mesure, rien ne s'oppose à ce qu'elle soit soumise au régime juridique correspondant. Aussi la cyberattaque commanditée à titre de rétorsion ne pourra-t-elle provoquer que des dommages limités, alors que celle qui constitue une contre-mesure devra notamment répondre au critère de proportionnalité et constituer, ce qui sera plus difficile à établir, le seul moyen d'action possible[22]. Pour les autres types de cyberattaques, en revanche, tant l'applicabilité que le sens des règles habituelles du droit international ne font guère l'objet de consensus en cas de cyberattaque. Pourtant, ils sont légion : le cas de figure le plus fréquent est bien celui d'actes isolés ou du moins non-inscrits dans le cadre d'un conflit armé, et que l'on peine à qualifier d' « agressions » au sens de la Charte des Nations Unies[23].

17 D'une manière plus générale, les principes de territorialité et le lien personnel, qui permettent de fonder habituellement les compétences de l'Etat, sont fréquemment invoqués pour appréhender internet par le biais du droit international[24]. Peuvent également s'avérer utiles les critères d'attribution de la responsabilité tels que l'implication d'un « organe de l'Etat »[25] dans la commission des actes de cyberguerre, en ce qu'ils permettent d'engager la responsabilité internationale d'un Etat à raison des agissements de ses agents publics dès lors qu'ils occasionnent un dommage. Mais les individus à l'origine de cyberattaques, loin d'être des agents officiels de cet Etat, sont bien plus souvent des ressortissants de l'Etat situés à l'étranger, voire des étrangers agissant depuis un autre territoire étatique. Ces critères s'avèrent donc, en eux-mêmes, insuffisants pour faire face à l'enjeu informatique.

18 Certes, le droit international comporte également des principes généraux qui permettent d'attribuer la responsabilité en matière de dommages transfrontières. Mais ceux-ci ne pourraient s'avérer utiles face aux cyberattaques que dans des circonstances particulières seulement, ce qui limite la portée de cette solution partielle. En effet, la responsabilité d'un Etat ne pourra être engagée sur le fondement de la jurisprudence *Fonderie de Trail* qu'en l'absence de faute avérée de l'Etat, et si tant est que le fait occasionnant le dommage ait pris pour point de départ le territoire de l'Etat[26]. Ainsi, le droit international général nous livre des clefs de lecture partielles et laisse des zones grises à l'heure d'appréhender un phénomène nouveau qui soulève de plus des difficultés de preuve sans précédent, se caractérise par sa dimension immatérielle, et présente une instantanéité difficile à saisir, ou du moins un rapport au temps particulier. Pour sa part, le droit international des droits de l'homme, grand oublié des études concernant les cyberattaques[27], s'avère de quelque utilité dans la recherche de règles et de raisonnements pertinents.

B – Les possibles apports du droit international des droits de l'homme

19 Puisque toutes les hypothèses ne sauraient être couvertes par le droit humanitaire et que le droit international général n'est que d'un recours partiel, le recueil de sources complémentaires dans le droit international des droits de l'homme s'avère opportun. En raison de son caractère plus général que le droit international humanitaire, de sa permanence[28], mais aussi de son objet, le droit international des droits de l'homme peut en effet s'avérer utile pour appréhender l'ensemble des phénomènes dits de cyberguerre et leurs conséquences à l'égard des individus. Ses instances ne rechignent guère à s'intéresser à des situations potentiellement régies par le droit humanitaire, ni même, d'ailleurs, à faire directement application de ses règles spéciales[29]. Elles pourraient d'ailleurs être conduites à connaître de cyberattaques et des violations des droits de l'homme consécutives. Les règles du droit international des droits de l'homme s'avèrent précieuses pour proposer des solutions juridiques les plus complètes et homogènes possibles, face à l'hétérogénéité réelle des situations de fait considérées ; par ce biais, un traitement juridique d'ensemble et un raisonnement général sur ces situations nouvelles peuvent être engagés. Ainsi, le droit international des droits de l'homme offre une grille de lecture nouvelle qui aide à affronter deux des difficultés juridiques principales auxquelles se heurte la cyberguerre : l'attribution de la

cyberattaque à un Etat et l'identification de règles de droit susceptibles de régir ses effets à l'égard des personnes physiques.

20 Le rattachement d'une cyberattaque à un Etat aux fins d'établissement de sa responsabilité constitue une difficulté première au soutien de laquelle on trouve quelques pistes de solution dans la protection internationale des droits de l'homme. En effet, la problématique de l'instantanéité d'une action susceptible de causer des dommages et, par conséquent, de générer la mise en cause de la responsabilité d'un Etat a également été posée en protection internationale des droits de l'homme. Elle a, devant les organes de protection régionale des droits de l'homme, donné lieu à des raisonnements à même d'aider à l'appréhension du phénomène.

21 Dans l'affaire *Banković* dont a eu à connaître la Cour européenne des droits de l'homme, le bombardement par les Forces alliées réunies sous l'égide de l'OTAN de la Radio-Televizije Serbije (RTS) a donné lieu à des discussions autour de la possibilité d'une juridiction extraterritoriale instantanée n'impliquant ni contact ni présence physique sur le territoire étranger. L'article 1er de la Convention européenne des droits de l'homme prévoit que « Les Hautes Parties contractantes reconnaissent à toute personne *relevant de leur juridiction* les droits et libertés définis au titre I »[30] ; la disposition s'interprète comme conjuguant une compétence principalement territoriale[31] et, par exception, une compétence en dehors du territoire. Les requérants soutenaient que la requête était « compatible *ratione loci* avec les dispositions de la Convention au motif que les actes incriminés, qui soit ont été accomplis en RFY, soit l'ont été sur le territoire des Etats défendeurs mais ont produit leurs effets en RFY, les ont fait entrer, eux et leurs proches décédés, dans la sphère de juridiction desdits Etats »[32]. Est ainsi invoquée, de façon subsidiaire et en vue de couvrir l'hypothèse d'un événement aérien de très brève durée, une conception extensive de la compétence territoriale. Elle permettait d'établir la juridiction d'un Etat dès lors qu'une décision – c'est-à-dire un fait causal immatériel – était adoptée depuis son territoire, et ce même si l'action consécutive devait se dérouler ailleurs, et prenait appui sur le d'ores et déjà établi mécanisme de la protection par ricochet[33]. Cet argument a été jugé peu convaincant par la Cour[34], qui a privilégié l'argumentation des Etats défendeurs. Ceux-ci rejetaient l'idée d'un contrôle suffisant pour caractériser la juridiction de l'Etat[35]. Ils liaient la reconnaissance d'une juridiction à l'existence d'une certaine durée de la relation, ainsi qu'à la mise en évidence d'une certaine forme d'allégeance à l'Etat ; en somme, il n'y aurait juridiction que lorsqu' « une forme de relation structurée existant pendant un certain laps de temps » pourrait être établie[36]. Les dangers d'une « théorie nouvelle de type causal »[37] ont ici été mis en avant par le juge, qui a rejeté cette argumentation[38]. La Cour souligne la nécessité de bien distinguer entre les deux conditions de recevabilité d'une requête que sont la question de savoir si l'intéressé peut être réputé victime d'une violation de droits garantis par la Convention, et la question de savoir si un individu relève de la juridiction d'un Etat partie au sens de la Convention. Elle nie la possibilité qu'une juridiction soit temporaire et de brève durée, et considère que l'exercice de pouvoirs publics sur le territoire étranger constitue une nécessité pour que la juridiction de l'Etat puisse être caractérisée au sens de la Convention[39]. En matière de cyberattaque, cet argument ne paraît pas dirimant : l'exercice ou l'obstruction à l'exercice normal des fonctions étatiques de manière temporaire constitue bien souvent la méthode employée par les cyberattaquants.

22 Que les arguments des requérants dans l'affaire *Banković* aient reçu un mauvais écho du côté de la Cour européenne des droits de l'homme à l'heure de proposer de nouveaux critères permettant de déclarer une requête recevable, et par conséquent de caractériser la responsabilité de l'Etat, est une chose. Qu'ils soient dépourvus de toute potentialité en serait une autre. D'ailleurs, la Commission interaméricaine des droits de l'homme a tenu un raisonnement similaire à celui du sieur Banković dans sa décision du 21 octobre 2010[40] . L'Equateur demandait que soit reconnue la possible responsabilité de la Colombie pour les préjudices causés à son ressortissant Franklin Guillermo Aisalla Molina, victime d'une exécution extrajudiciaire conduite par les forces de sécurité colombiennes dans le cadre de l'« Opération Phoenix » menée le 1er mars 2008 en territoire équatorien. La Commission a recherché l'existence d'un lien de causalité entre l'atteinte aux droits de l'homme occasionnée et la conduite extraterritoriale de l'Etat : « *At the time of examining the scope of the American Convention's jurisdiction, it is necessary to determine whether there is a causal nexus between the extraterritorial conduct of the State and the alleged violation of the rights and freedoms of an individual* »[41].

23 Au-delà de cette dimension causale de l'engagement de la responsabilité, partiellement admise en protection internationale des droits de l'homme, le caractère instantané du contrôle requis aux fins d'engagement de la responsabilité d'un Etat paraît plus facilement reconnu. En effet, l'on trouve des décisions d'organes de protection internationale des droits de l'homme qui permettent, en l'absence d'une présence matérielle s'étalant sur une longue durée, l'engagement de la responsabilité d'un Etat contrôlant effectivement des événements se déroulant sur le territoire d'un autre Etat. La théorie du « contrôle global » fait référence en des termes généraux à l'autorité et au contrôle de l'Etat non territorial comme à autant de critères décisifs aux fins d'établir sa juridiction et donc de pouvoir engager sa responsabilité[42]. De façon plus spécifique, dans l'affaire *Stocké*, ce sont l'« *actual authority and responsibility* »[43] qui sont considérés comme décisifs. Le contrôle requis pourrait ainsi n'être qu'instantané, l'essentiel étant que l'autorité exercée par l'Etat soit effective en un instant *T*[44].

24 Ainsi, toute juridiction n'est pas territoriale, loin s'en faut. Comme l'a d'ailleurs précisé le Comité des droits de l'homme, dans un raisonnement par la suite cité par la Commission interaméricaine, « *the qualification 'subject to its jurisdiction', contained in article 29(1) of the Covenant, does not refer to the place where the violation occurs but to the relationship between the individual and the State concerned* »[45]. Ainsi, suivant une logique non territoriale, une approche mettant en avant un rattachement humain pourrait s'avérer plus utile pour consacrer la responsabilité d'un Etat en raison d'une cyberattaque affectant les civils et portant atteinte à leurs droits de l'homme[46].

25 L'idée qu'un exercice instantané de la souveraineté sur des individus serait susceptible de déclencher la responsabilité de l'Etat pour violation des droits de l'homme s'avère particulièrement intéressante pour traiter des cas de cyberattaques. L'instantanéité du phénomène se conjugue en effet à son absence de véritable ancrage territorial pour présenter d'importants points communs avec l'hypothèse de cyberattaques menées contre un Etat et affectant fort probablement les individus se trouvant sur son territoire et leurs droits de l'homme (pour exemple : droit à une vie privée, droits sociaux, etc.).

26 Enfin, force est de constater que les droits de l'homme eux-mêmes, tels qu'ils sont reconnus par les textes internationaux, peuvent être d'une grande utilité pour

appréhender les cyberattaques. Droit à la vie, droit à la vie privée, intégrité physique, nombreux sont les droits auxquels une attaque informatique peut porter atteinte. Ces droits bénéficiant d'une protection permanente sur le fondement de textes internationaux, les victimes auront tout intérêt, en cas de dommage(s), à prendre appui sur le droit international des droits de l'homme et ses organes plutôt qu'à attendre une protection du droit humanitaire. Ce dernier est en effet applicable uniquement en temps de conflit armé et n'est susceptible de n'engager la responsabilité des Etats que dans ces seules situations, ou bien d'engager la responsabilité d'individus déterminés lorsque les infractions commises par eux, d'une gravité suffisante, constitueront également des crimes au sens du droit international pénal. Dans un tel contexte, les organes de protection internationale des droits de l'homme ont tout intérêt à se saisir de la problématique des cyberattaques et à affiner les techniques permettant de faciliter l'accès à leur forum comme la reconnaissance de la responsabilité des Etats commanditaires de tels agissements.

NOTES

1. On peut relever : B. Smith, « An Eye for an Eye, A Byte for a Byte », *Federal Lawyer*, October 1995, pp. 12-13 ; M.N. Schmidt, « Computer Network Attack and the Use of Force in International Law : Thoughts on a Normative Framework », *Columbia Journal of Transnational Law*, 1999, pp. 885-937 ; *Air Force Law Review*, 2009, n°64 (n° spécial) ; L. Swanson, « The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Geogian Cyber Conflict », *Loyola of Los Angeles International and Comparative Law Review*, 2010, pp. 303-333 ; XXXIV^{ème} Table ronde sur les sujets actuels du droit international humanitaire, San Remo, 8-10 septembre 2011 ; XXXI^{ème} Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, Suisse, 28 novembre – 1er décembre 2011, *Le droit international humanitaire et les défis posés par les conflits armés contemporains. Rapport*, CICR, 31IC/11/5.2, 2011, 61 p. ; H. Lin, « Operational Reality of Cyber Warfare », *IIHL* 2011, pp. 137-143 ; D. J. Ryan et alii, « International Cyberlaw : A Normative Framework », *Georgetown Journal of International Law*, 2011, pp. 1161-1197 ; M. Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », Politique étrangère, vol. 77, été 2012, n°2, pp. 305-316 ; J.-M. Bockel, Commission des Affaires étrangères, de la Défense et des Forces Armées, Sénat, « La Cyberdéfense : un enjeu mondial, une priorité nationale », Rapport d'information n°681 (2011-2012), 18 juillet 2012 ; M. Hecker et T. Rid, « Les armées doivent-elles craindre les réseaux sociaux ? », *Politique étrangère*, vol. 77, été 2012, n°2, pp. 317-328 ; H. Lin, « Cyber Conflict and International Humanitarian Law », *RICR*, 2012, vol. 886, pp. 515-532 ; J. Richmond, « Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict ? », *Fordham International Law Journal*, March, 2012, pp. 843-894 ; L. Simonet, « L'usage de la force dans le cyberespace et le droit international », *Revue de défense nationale*, 2012, pp. 51-55 ; M.N. Schmidt, « International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed », *Harvard International Law Journal* vol. 54, Dec. 2012, pp. 13-37 ; M.N. Schmidt (dir.), *Tallinn Manual on the International Law Applicable to*

Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge UP, 2013, 282 p. ; University of Pensylvannia, Roundtable on Cyberwar and the Rule of Law, 2012, consultable sur : https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/schedule.php ; K. Ziolkowki, « Stuxnet : Legal Considerations », *Humanitäres Völkerrecht*, vol. 25, 2012, pp. 39-147 ; J. Goldsmith, « How Cyber Changes the Laws of War », *EJIL* 2013, vol. 24, n°1, pp. 129-138 ; Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, 2014, pp. 323 et s.

2. Sur ces questions, voir notamment : D. Brown, « A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict », *Harvard International Law Journal*, 2006, pp. 179-221 ; Ch. Dodge, « United States Cyber Command : International Restrictions vs. Manifest Destiny », *North Carolina Journal of Law & Technology Online Edition*, 2010, pp. 1-27.

3. L. Swanson recense trois catégories d'armes informatiques : 1) « Syntactic weapons, which target a computer's operating system, include malicious code, such as viruses, worms, Trojan Horses, DdoS, and spyware » ; 2) « semantic weapons [which] consist of altering information that enters the computer's system » ; 3) « mixed or blended weapons [which] combine sysntactic and semantic weapons to attack both information and the computer's operating system, resulting in a more sophisticated attack » (source : L. Swanson, « The Era of Cyber Warfare : Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict », *Loyola of Los Angeles International and Comparative Law Review*, 2010, pp. 310-311).

4. Th. Rid, « Cyber War Will not Take Place », *Journal of Strategic Studies,* vol. 35, n°1, octobre 2011 ; M. Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, 2012, vol. 2, pp. 305-316.

5. Voir *CBS this Morning. 60 mn investigates cyberwarfare*, Interview en date du 5 mars 2012, à propos de Stuxnex.

6. Sur le rôle d'internet dans le Jihad, par exemple, voir : W. Adhami, « The Strategic Importance of the Internet for Armed Insurgent Groups in Modern Warfare », *RICR*, vol. 89, n°868, 2007, p. 864.

7. Aussi le Lieutenant Colonel Joshua E. Kasterberg considère-t-il que les attaques menées contre la Géorgie en 2008, usuellement présentées comme des actes de cyberguerre, seraient qualifiées d'« infractions » sur le fondement de la Convention du Conseil de l'Europe sur la cybercriminalité (E. Kastenberg, « Non-Intervention and Neutrality in Cyberspace, An Emerging Principle in the National Practice of International Law », *Air Force Law Review*, 2009, vol. 64, p. 58.

8. Voir par exemple : M. Bettati, *Droit humanitaire*, Précis Dalloz, 2012, p. 29.

9. TPIY *Procureur c. Tadić*, IT-94-AR 72, 2 octobre 1995, § 10.

10. Sur ce dernier aspect : S Vité, « La lutte contre la criminalité organisée : peut-on parler de conflit armé au sens où l'entend le droit international humanitaire ? », *Conflits armés, parties aux conflits armés et droit international humanitaire : les catégories juridiques face aux réalités contemporaines,* Actes du colloque de Bruges, 22-23 octobre 2009, *Collegium*, n°40, 2010, pp. 69-77.

11. V.M. Antolin-Jenkins, « Defining the Parameters of Cyberwar Operations : Looking for Law in All the Wrong Places ? », *Naval Law Review*, 2005, p. 134.

12. V.M. Antolin-Jenkins, *ibid.*, « The more critical question is whether it is reasonable to require adherence to old concepts of what constitutes "use of force" when it is clear that the destructive power of cyberspace operations can threaten the economic integrity of a state », p. 172.

13. M. Dunn Cavelty, « Cyberwar: Concept, Status Quo, and Limitations », CSS Analysis in Security Policy, n° 71, avril 2010, <www.sta.ethz.ch/CSS-Analysis-in-Security-Policy/CSS-Analysis-in-Security-Policy-Archive/No.-71-Cyberwar-Concept-Status-Quo-and-Limitations-April-2010>, consulté le 1er juillet 2014.

14. Convention sur la cybercriminalité, Budapest, 23 juin 2001, STE n°185.

15. La question du possible recours à la qualification d'agression pour désigner les actes de cyberguerre a d'ores et déjà fait l'objet d'une littérature assez abondante ; voir par exemple : N. Weisbord, « Conceptualizing Aggression », *Duke Journal of Comparative & International Law*, 2009, pp. 1-68 ; J. Kulesza, « State Responsibility for Cyberattacks on International Peace and Security », *Polish Yearbook of International Law*, 2010, pp. 139-152 ; et, plus largement sur le recours à la force et la cyberguerre : *Max Planck UNYB*, vol. 14, 2010, pp. 85-130.

16. Comité international de la Croix-Rouge, *Le droit international humanitaire et les défis posés par les conflits armés contemporains. Rapport*, XXXI[ème] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, Suisse, 28 novembre-1[er] décembre 2011, 31IC/11/5.1.2, p. 42.

17. Voir par exemple : *Le droit et l'immatériel*, *APD* t. 43, 1999 ; A.-T. Norodom, « Propos introductifs. Internet et le droit international : défi ou opportunité ? », dans : Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, 2014, pp. 11 et s.

18. Voir : M.N. Schmidt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*, Cambridge UP, 2013, *spéc.* pp. 15 et s.

19. Sur ces questions, voir par exemple : K. Dörmann, « Applicability of the Additional Protocols to Computer Network Attacks », International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 novembre 2004, http://www.icrc.org/eng/resources/documents/misc/68lg92.htm ; V.M. Antolin-Jenkins, « Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places ? », *Naval Law Review*, 2005, pp. 132-173 ; L. Swanson, « The Era of Cyber Warfare Applying Internaitonal Humanitarian Russian-Georgian Cyber Conflict », *Loyola of Los Angeles International and Comparative Law Review*, Spring 2010, pp. 303-333 ; Interview de C. Droege, Conseillère juridique du CICR, le 16-08-2011, « Pas de vide juridique dans le cyberespace », http://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm ; H. Lin, « Cyber Conflict and International Humanitarian Law », *RICR* vol. 94, n°886, 2012, pp. 515-531 ; J. Richmond, « Does Stuxnet Demonstrate a Need for Modifications of the Law of Armed Conflict ? », dans : *Cyber Attacks : International Cybersecurity in the 21st Century*, *Fordham International Law Journal*, March, 2012 ; J. Goldsmith, « How cyber changes the laws of war », *EJIL* 2013, vol. 24-1, pp. 129-138 ; L. Baudin, *Les cyberattaques dans les conflits armés*, Coll. Le droit aujourd'hui, L'Harmattan, 2014, 252 p.

20. E. David, *Principes de droit des conflits armés*, 5[ème] éd., Bruxelles, Bruylant, 2012, p. 78.

21. Sur ces questions, voir par exemple : M.N. Schmitt, « Computer Network Attack and the Use of Force in International Law : Thoughts on a Normative Framework », *Columbia Journal of Transnational Law*, 1999, pp. 885-936 ; M. Roscini, « World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force », *Max Planck UNYB*, 2010, pp. 85-130.

22. Tribunal arbitral germano-portugais, *Affaire de Lysne (Responsabilité de l'Allemagne à raison des actes commis postérieurement au 31 juillet 1914 et avant que le Portugal ne participât à la guerre*), *RSA* II, p. 1056.

23. Sur la question de la qualification d'agression pour les actes de cyberguerre, voir *supra*, note n° 16.

24. Sur ces questions, voir : M.N. Schmidt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare..., op. cit.* : « RULE 2 – JURISDICTION. Without prejudice to applicable international obligations, a State may exercise its jurisdiction : (a) over persons engaged in cyber activities on its territory ; (b) over cyber infrastructure located on its territory, and (c) extraterritorially, in accordance with international law ». Voir également : Ph. Lagrange, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'Internet à un droit international du cyberespace ? », dans : Colloque de la S.F.D.I., Rouen, *Internet et le droit international*, Paris, Pedone, 2014 ; A.-T. Norodom, « Propos introductifs... », *ibid.*, pp. 28 et s.

25. Les articles 4 et 5 du Projet d'articles de la Commission du droit international sur la responsabilité de l'Etat traitent ainsi de l'engagement de la responsabilité de l'Etat du fait des actes de ses démembrements, c'est-à-dire de toute collectivité territoriale ou entité « habilitée par le droit de cet Etat à exercer des prérogatives de la puissance publique » (C.D.I., *Projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite*, 2001, dans : Documents officiels de l'Assemblée générale, 56ème session, Supplément n° 10 (A/56/10).).

26. Sentence arbitrale, *Fonderie de Trail*, 11 mars 1941, *R.S.A.* III, p. 907.

27. La problématique de l'articulation entre droits de l'homme et cyber attaques ou cyberguerre est habituellement exclue des études doctrinales ; pour exemple : M.N. Schmidt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*..., *op. cit.*, p. 4.

28. AGNU, *Déclaration sur les relations amicales entre les Etats*, Résolution 2675 (XXV), 24 octobre 1970, § 1 : « les droits fondamentaux de l'homme (...) demeurent pleinement applicables en cas de conflit armé » ; CIJ Avis consultatif sur la *Licéité de la menace ou de l'emploi d'armes nucléaires* 1996 : les droits de la personne s'appliquent ou doivent en tous cas être pris en compte dans la mise en œuvre du droit des conflits armés.

29. Suite à l'intervention américaine à La Grenade (1983), la Commission interaméricaine des droits de l'homme s'est par exemple déclarée compétente pour traiter d'une plainte introduite suite au bombardement d'un asile d'aliénés dans lequel des pensionnaires avaient été tués ou blessés (IACHR, *Disabled People's International et al.* v. *US*, Decision of the Commission as to the Adminssibility, OEA/Ser.L/V/II.71, Doc. 9 rev. 1, 22 September 1987, pp. 184-192). La Cour EDH quant à elle considéré sous l'angle de la Convention des espèces relatives à la situation en Tchétchénie (pour exemple : Cour EDH, *Pitsayeva et autres c. Russie*, 9 janvier 2014, n° 53036/08 et autres).

30. Italiques ajoutés.

31. Cour EDH (Grande Chambre), *Al-Skeini et autres c. Royaume-Uni*, 7 juillet 2011, n° 55721/07, § 131 ; Cour EDH, (Grande Chambre), 19 décembre 2001, *Banković et autres c. Belgique et 16 autres Etats membres*, Décision d'irrecevabilité, 12 décembre 2001, n° 52207/99, § 59 ; Cour EDH, *Al-Dulimi et Montana Management Inc c. Suisse*, n° 5809/08, 26 novembre 2013.

32. Cour EDH, (Grande Chambre), 19 décembre 2001, *Banković...*, *ibid.*, § 30.

33. *Ibid.*, § 53.

34. *Ibidem*, § 77.

35. *Ibidem*, § 44.

36. *Ibidem*, § 36.

37. *Ibidem*, § 43.

38. Dans le même sens, voir également : Cour EDH (Grande Ch.), *Medvedyev c. France*, 29 mars 2010, n° 3394/03, § 64 ; Cour EDH, *Hirsi Jamaa et a. c. Italie*, 23 février 2012, n° 27765/09, § 73.

39. Cour EDH, (Grande Chambre), 19 décembre 2001, *Banković...*, *ibid.*, § 71.

40. Commission IADH,Inter-state petition IP-02, Admissibility, *Franklin Guillermo Aisalla Molina*, *Ecuador – Colombia*, 21 octobre 2010.

41. *Ibid.*, § 99.

42. Cour EDH, *Loizidou c. Turquie*, 23 mars 1995, n°15318/89, § 56 ; Cour EDH, *Issa and others v. Turquie*, 30 mars 2005, n° 31821/96, § 71 ; CEDH, *Andreas Manitaras and others v. Turkey*, 3 June 2008 n° 54591/00, §§ 27-28 ; Cour EDH, *Ilascu et a. c. Moldova et Russie*, 8 juillet 2004, n° 48787/99, § 315.

43. Commission EDH, *Stocké v. Germany*, 12 October 1989, Series A, vol. 1999, 24, § 88.

44. Le caractère effectif du contrôle est décisif pour emporter juridiction extraterritoriale de l'Etat : voir par exemple le raisonnement du Comité contre la torture concernant Israël dans : GAOR, 64th sess, Suppl. No. 44. En faveur d'une interprétation contextuelle, pour chaque cas d'espèce, du caractère effectif de ce contrôle, voir : M. Scheinin « Extraterritorial Effect of the

international Covenant on Civil and Political Rights », dans : F. Coomans, M.T. Kamminga (dir.), *Extraterritorial Application of Human Rights Treaties*, Oxford, Intersentia, 2004, pp. 73 et s., *spéc.* p. 76.

45. Commission IADH, *Affaire 10.675 c. Etats-Unis (Haitian Interdiction Case)*, 13 mars 1997, § 141.

46. Dans ce sens, voir notamment : R. Lawson, « Life After *Banković* : On the Extraterritorial Application of the European Convention on Human Rights », dans : F. Coomans, MT Kamminga (dir.), *Extraterritorial Application of Human Rights Treaties*, Oxford, Intersentia, 2004, *spéc.* p. 98.

ABSTRACTS

The terminology "Cyberwar" lacks precision: the realities it covers, thus manifolds, are not limited to armed conflict situations. "Cyberwar" raises many questions of international law that cannot be all dealt with *jus in bello* rules, and thus needs further investigations in other fields of international law such as international human rights law.

Qu'est-ce au juste que la cyberguerre, et quelles questions pose-t-elle au droit ? L'expression « cyberguerre » est manifestement trop restrictive eu égard à la variété des contextes dans lesquels s'inscrivent les attaques informatiques. Dès lors, les règles du *jus in bello* ne sauraient à elles seules permettre d'appréhender un phénomène hétéroclite qui ne se limite pas aux situations de conflit armé, et un recours à d'autres branches du droit, tel le droit international des droits de l'homme, s'avère utile.

INDEX

Mots-clés: Cyberguerre – cyberattaque - droit international humanitaire - juridiction de l'Etat
Keywords: Cyberwar – cyberattack - humanitarian law - State jurisdiction